

Controllo Logico

I controlli d'accesso logico devono fornire un modo tecnico per controllare l'accesso di un utente alle risorse di sistema ed alle informazioni al fine di garantire il controllo delle informazioni che gli utenti possono utilizzare, dei programmi che possono eseguire e delle modifiche che possono apportare.

Nella stesura delle procedure si deve tener conto che:

- L'accesso è la capacità da parte di un soggetto (utente o processo) di fare operazioni (lettura, aggiornamento, scrittura, comunicazione) che accedono e usano "oggetti" (applicazioni, programmi, dati).
- L'autorizzazione è il permesso per usare una risorsa del computer. L'autorizzazione è assegnata, direttamente o indirettamente, dal proprietario del sistema o dell'applicazione.
- L'autenticazione dimostra che gli utenti sono chi sostengono di essere.
- Il controllo d'accesso è strettamente legato all'autenticazione.

I controlli d'accesso logici devono contribuire a proteggere:

- I sistemi operativi e l'altro software di sistema dalla modifica o dalla manipolazione non autorizzata (e quindi contribuire ad accertare l'integrità e la disponibilità del sistema).
- L'integrità e la disponibilità delle informazioni limitando il numero di utenti e di processi con accesso.
- Le informazioni confidenziali dalla rilevazione agli individui non autorizzati.

Deve essere controllato il diritto d'accesso che si permette, ovvero quali sono i privilegi assegnati alle risorse in funzione del ruolo che ricoprono (per esempio la capacità per l'utente di eseguire, ma di non cambiare, i programmi di sistema, di leggere i files senza poterli riscrivere o cancellare, ecc).

Il servizio di identificazione ed autenticazione deve essere eseguito mediante tecniche basate su *password* e *userid* (identificativo utente); relativamente alla *userid* si fa riferimento alle norme previste dalla legge 675/96 e relativo DPR 318.

Tutti gli utenti interni e esterni che lavorano con continuità sui sistemi dell'Amministrazione, devono essere dotati di un proprio *userid* personale, mentre gli utenti esterni dovranno utilizzare, secondo i casi, un *userid* che identifica la persona, il ruolo o l'ente. In ogni caso è